

AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions and listings of claims in the application.

LISTING OF CLAIMS

1-15 (Canceled)

16. (New) A method for securing access to a content , encrypted by an encryption key , transmitted from a broadcaster to a plurality of multimedia units, each of which is associated with a security module comprising at least one unique authorisation key and at least two group authorisation keys, said method allowing the broadcaster to selectively revoke access rights from at least one of said security modules, this method involving the organisation of said security modules into a hierarchical tree of at least two levels of groups, the first of said levels comprising a plurality of security modules which share a common group authorisation key, the second of said levels comprising at least two groups of the first level groups of security modules each sharing a further common group key, said method comprising the following steps:

- generation of a temporary encryption key,
- generation of a value allowing the determination of the encryption key of the content ,
- encryption under the temporary encryption key of said value,
- transmission of the encrypted value to the plurality of security modules,
- transmission of the content, encrypted under the encryption key , to the plurality of security modules,
- encryption and transmission of at least two cryptograms each comprising the temporary encryption key , the first cryptogram being encrypted under the unique authorisation key of a non-revoked security module and the second cryptogram being encrypted by a group authorisation key pertaining to a group of security modules to which the revoked security module does not belong,
- decryption, by at least one of the non-revoked security modules, of at least one of the plurality of cryptograms using either one of the group authorisation keys or the unique authorisation key to give the temporary encryption key ,

- decryption, by at least one of the non-revoked security modules, of the encrypted value using the temporary encryption key to give the encryption key ,
- decryption, by the multimedia unit associated with at least one non-revoked security module, of the encrypted content using the encryption key to get clear content .

17. (New) Method according to claim 16, wherein said value allowing the determination of the encryption key of the content is the encryption key itself.

18. (New) Method according to claims 16, wherein said value allowing the determination of the encryption key of the content includes at least one variable element and said encryption key is built from this variable element.

19. (New) Method according to claim 17, wherein said value allowing the determination of the encryption key of the content includes at least one variable element and said encryption key is built from this variable element.

20. (New) Method according to claim 18, wherein said value allowing the determination of the encryption key furthermore includes an additional element related to the content in addition to the variable element.

21. (New) Method according to claim 20, wherein said additional element contains conditions of access to the transmitted content.

22. (New) Method according to claim 18, wherein said encryption key is built by means of a hash function applied at least to said variable element.

23. (New) Method according to claim 20, wherein said encryption key is built by means of a hash function applied at least to said variable element.

24. (New) Method according to claim 21, wherein said encryption key is built by means of a hash function applied at least to said variable element.

25. (New) Method according to any of the claims 18, wherein said encryption key is built by means of an encryption function applied at least to said variable element.

26. (New) Method according to any of the claims 20, wherein said encryption key is built by means of an encryption function applied at least to said variable element.

27. (New) Method according to claim 21, wherein said encryption key is built by means of an encryption function applied at least to said variable element.

28. (New) Method for securing access to a content , encrypted by an encryption key , transmitted from a broadcaster to a plurality of multimedia units, each of which is associated with a security module comprising at least one unique authorisation key and at least two group authorisation keys, said method allowing the broadcaster to selectively revoke access rights from at least one of said security modules, this method involving the organisation of said security modules into a hierarchical tree of at least two levels of groups, the first of said levels comprising a plurality of security modules which share a common group authorisation key, the second of said levels comprising at least two groups of the first level groups of security modules each sharing a further common group key, said method comprising the following steps:

- generation of a temporary encryption key ,
- generation of a value allowing the determination of the encryption key of the content ,
- transmission of said value to the plurality of security modules,

- transformation, under the temporary encryption key , of the value allowing the determination of the encryption key of the content, this transformation giving as a result, said encryption key of the content,
- transmission of the content, encrypted under the encryption key , to the plurality of security modules,
- encryption and transmission of at least two cryptograms each comprising the temporary encryption key , the first cryptogram being encrypted under the unique authorisation key of a non-revoked security module and the second cryptogram being encrypted by a group authorisation key pertaining to a group of security modules to which the revoked security module does not belong,
- decryption, by at least one of the non-revoked security modules, of at least one of the plurality of cryptograms using either one of the group authorisation keys or the unique authorisation key to give the temporary encryption key ,
- decryption, by at least one of the non-revoked security modules, of the encrypted value using the temporary encryption key to give the encryption key ,
- decryption, by the multimedia unit associated with at least one non-revoked security module, of the encrypted content using the encryption key to get clear content .

29. (New) Method according to claim 28, wherein said value allowing the determination of the encryption key of the content includes at least one variable element and said encryption key is built from this variable element.

30. (New) Method according to claim 29, wherein said value allowing the determination of the encryption key further includes an additional element in addition to the variable element .

31. (New) Method according to claim 30, wherein said additional element contains the conditions to access to the transmitted content .

32. (New) Method according to claim 28, wherein the transformation is a hash operation with a key, the key being the temporary encryption key.

33. (New) Method according to claim 16, wherein the authorization keys are classified in levels, the keys of the highest level being unique and individual for one security module, the key of the lowest level being known by all the security modules and the intermediate level keys being common to a security module subset, this subset not containing all the modules.

34. (New) Method according to claim 33, intended for the revocation of at least one security module, wherein, as a second authorization key intended for the encryption of the temporary key, the keys common to the largest possible group of security modules are used, this group not including the at least one revoked security module.

35. (New) Method according to claim 33, wherein a message is sent to the security modules, indicating the level of the authorization key which must be used.